

10-02-00

A

UNITED STATES CONTINUING UTILITY PATENT APPLICATION
under 37 C.F.R. § 1.53(b)

Page 1

Atty. Docket No. 03797.85750

jc916 U.S. PTO
09/29/00
Barcode

CERTIFICATE OF EXPRESS MAILING UNDER 37 C.F.R. § 1.10: The undersigned hereby certifies that this United States Patent Application and all papers noted herein as being attached, are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" Service under 37 C.F.R. § 1.10 today, **September 29, 2000**, and is addressed to: Assistant Commissioner for Patents, Washington, D.C. 20231.

Express Mail Label No.: EL 625292249 US

Assistant Commissioner for Patents
Box Patent Applications
Washington, D.C. 20231

Enclosed herewith is a continuing patent application and the following papers:

First Named Inventor (or application identifier): Georgios Chrysanthakopoulos

Title of Invention: Method and Apparatus of Remote Computer Management

- Continuation
- Divisional
- Continuation-in-Part

of prior application No. 09/515,424, filed February 29, 2000.

1. Specification 21 pages (including specification, claims, abstract) / 25 claims (4 independent)
2. Declaration/Power of Attorney:
 - Copy from Prior Application (for continuation or divisional application)
 - Newly Executed Declaration (for CIP application)
 - Deferred under 37 C.F.R. § 1.53(f)
 - Deletion of Inventor(s) - Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b)
 - Incorporation by Reference - The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied is considered as being part of the disclosure of the accompanying application and is hereby incorporated by reference therein
3. 4 Distinct sheets of Informal Drawings.
4. Preliminary Amendment
5. Information Disclosure Statement

UNITED STATES CONTINUING UTILITY PATENT APPLICATION
under 37 C.F.R. § 1.53(b)

Page 2

Atty. Docket No. 03797.85750

- Form 1449
- A copy of each cited prior art reference

6. Assignment

- Assignment with Cover Sheet attached
- Assignment filed in prior application. Application assigned to:

7. Priority is hereby claimed under 35 U.S.C. § 119 based upon the following application(s):

Country	Application Number	Date of Filing (day, month, year)
U.S.A.	09/515,424	29 February 2000
U.S.A.	60/169,718	08 December 2000

8. Priority document(s)

9. Small Entity Statement

- Small Entity Statement was filed in prior application, Small Entity Status is still proper and desired
- is attached
- is no longer claimed

10. Microfiche Computer Program (Appendix)

11. Nucleotide and/or Amino Acid Sequence Submission

- Computer Readable Copy
- Paper Copy (identical to computer copy)
- Statement verifying identity of above copies

UNITED STATES CONTINUING UTILITY PATENT APPLICATION
under 37 C.F.R. § 1.53(b)

Page 3

Atty. Docket No. 03797.85750

12. Calculation of Fees:

FEES FOR	EXCESS CLAIMS	FEE	AMOUNT DUE
Basic Filing Fee (37 C.F.R. § 1.16(a))			\$690.00
Total Claims in Excess of 20 (37 C.F.R. § 1.16(c))	5	18.00	\$90.00
Independent Claims in Excess of 3 (37 C.F.R. § 1.16(b))	1	78.00	\$78.00
Multiple Dependent Claims (37 C.F.R. § 1.16(d))	6	260.00	\$0.00
Subtotal - Filing Fee Due			\$858.00
		MULTIPLY BY	
Reduction by 50%, if Small Entity (37 C.F.R. §§ 1.9, 1.27, 1.28)	0		\$0.00
TOTAL FILING FEE DUE			\$858.00
Assignment Recordation Fee (if applicable) (37 C.F.R. § 1.21(h))	1	40.00	\$40.00
GRAND TOTAL DUE			\$898.00

13. PAYMENT is:

included in the amount of the GRAND TOTAL by our enclosed check. A general authorization under 37 C.F.R. § 1.25(b), second sentence, is hereby given to credit or debit our Deposit Account No. 19-0733 for the instant filing and for any other fees during the pendency of this application under 37 C.F.R. §§ 1.16, 1.17 and 1.18

not included, but deferred under 37 C.F.R. § 1.53(f).

14. All correspondence for the attached application should be directed to:

Pamela I. Banner
Banner & Witcoff, Ltd.
1001 G Street, N.W., 11th Floor
Telephone: (202) 508-9100
Facsimile: (202) 508-9299

15. Other: Return Postcard

Date: September 29, 2000

By: Christopher P. Moreno
Christopher P. Moreno
Reg. No. 38,566

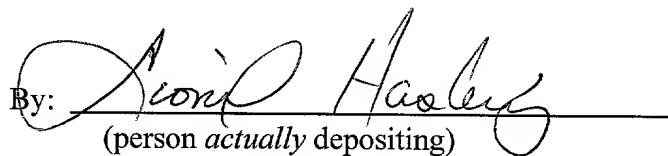
CPM/cla

**CERTIFICATE OF MAILING BY "EXPRESS MAIL"
(PATENT)**

Express Mail No. EL 625292249 US

Deposited September 29, 2000

I hereby certify that the attached correspondence, identified below, is being deposited with the United States Postal Service as "Express Mail Post Office to Addressee" under 37 CFR § 1.10 on the date indicated above and is addressed to: BOX PATENT APPLICATIONS, Assistant Commissioner for Patents, Washington, D.C. 20231.

By: 
(person *actually* depositing)

In the Application of: Georgios Chrysanthakopoulos, Pasquale DeMaio, and Valerie R. See

Filing Date: September 29, 2000

For: METHOD AND APPARATUS OF REMOTE COMPUTER MANAGEMENT

- (X) 37 C.F.R. §1.53(b) Transmittal Letter (in duplicate)
- (X) Specification - 14 pages of description; 6 pages of claims (25 claims/4 independent) and 1 page abstract
- (X) Four (4) Distinct Sheets of Informal Drawings
- (X) Information Disclosure Statement
- (X) PTO Form-1449 with Five (5) Cited References
- (X) Joint Declaration for Patent Application (3 pages)
- (X) Recordation Form Cover Sheet (in duplicate) with Attached Assignment (3 pages)
- (X) Filing Fee Check No. 073946 in the amount of \$898.00
- (X) Return Receipt Postcard

Attorney Docket No: 03797.85750

METHOD AND APPARATUS OF REMOTE COMPUTER MANAGEMENT

Technical Field

5 The present invention relates generally to computer management techniques and, in particular, to a method and apparatus for remote computer management.

Cross-Reference To Related Applications

This application is a continuation-in-part of U.S. Patent Application Serial No.

10 09/515,424 entitled "METHOD AND APPARATUS FOR PROVIDING SECURE REMOTE DEBUGGING OF COMPUTER SOFTWARE OVER A SERIAL BUS," filed on February 29, 2000, which is a continuation-in-part of U.S. Patent Application Serial No. 09/488,015 entitled "METHOD AND APPARATUS FOR REMOTELY DEBUGGING COMPUTER SOFTWARE OVER A SERIAL BUS," filed on January 20, 2000, both assigned to the same assignee of the present invention. Furthermore, priority is claimed to U.S. Provisional Patent Application No. 60/169,718, filed on December 8, 1999.

Background Of The Invention

Techniques for performing remote management of computers are well known in the art.

20 Remote management generally refers to the operational control of a given computer by another, remotely located computer. Examples of such control include, but are not limited to, configuring software, re-boot operations, status determination of field-replaceable units (FRUs), diagnostic procedures, firmware downloading, keyboard/video/mouse redirections, configuring the operating system, etc. Some management commands are of value when the computer being managed does not have a fully functioning operating system installed that would typically provide the mechanisms for managing the computer. This requires specialized mechanisms for controlling the computer that don't require the operating system to be fully functioning.

In many systems, computers to be managed are coupled via local area networks (LANs), serial data links or modems to a managing entity, such as a remotely located management terminal (e.g., another computer). Point-to-point links, such as so-called RS-232 serial links, are typically dedicated for this purpose and are therefore subject to more direct control by an operator of the system thereby allowing physical security to be implemented and making logical security less of a concern. However, RS-232 serial connections are limited in distance and to point-to-point connections. Additionally, these point-to-point links typically exist apart from the network connections used to convey other types of traffic between the computer being managed and other computers. Other forms of networked communication, such as LAN, wide area networks (WAN) and IEEE 1394 (absent the teachings of the present invention), allow greater distance connectivity choices but require complicated logical security and cannot support general communication simultaneously, requiring additional special purpose communication hardware.

Such techniques are further limited. For example, while it is possible using these techniques for the remote computer to access key components including memory and memory-mapped devices (i.e., memory accessed by software, such as operating systems, memory mapped hardware devices to be managed and service processors) of the computer being controlled, the process is generally very difficult requiring complex and non-standardized hardware. Generally, in such systems, the computer's processor must act as an intermediary between the component under consideration and a remote management entity, thereby diminishing the reliability of management commands. However, other types of communication links are capable of providing such direct access to key computer components. For example, the IEEE 1394 serial bus allows a remote computer to directly access internal computer components without the intervention of the computer's processor. Furthermore, this remote access does not prevent general communication on the 1394 serial bus, which requires simultaneous use of the computer's processor. For this reason, the IEEE 1394 serial bus represents an attractive option for use in remote computer management. (The IEEE 1394 serial bus standard is based largely upon the internationally adopted ISO/IEC 13213 (ANSI/IEEE 1212) CSR Architecture Specification and the IEEE 1394-1995 Serial Bus Specification.)

Although technologies that allow more direct access to a computer's components, such as IEEE 1394 serial bus technology, can be used to advance remote computer management techniques, such techniques do raise security concerns. That is, any communication link that provides a remote management terminal access to a given computer's components may also be exploited by other devices to gain access. For example, it may be possible for any device coupled to the IEEE 1394 serial bus to similarly gain access to a given computer's internal components. Similar security concerns arise with other networking technologies, such as "ETHERNET" networks. These security holes represent a significant impediment to the use of such technology in the area of remote computer management. Thus, a technique that overcomes such security concerns in the context of remote computer management would represent advancement in the art.

Summary Of The Invention

The present invention overcomes the limitations described above by providing a technique whereby only authorized devices are allowed to provide management commands to a computer being controlled. In particular, the computer being controlled is coupled via a management port to a communications bus that is in turn coupled to at least one other device comprising one or more authorized management devices. Only management commands received from authorized management devices via the management port may be executed or otherwise responded to. Other devices coupled to the communication bus but not to the management port cannot be an authorized management device, and any management commands received from such devices are ignored. In a preferred embodiment, the communication bus comprises an IEEE 1394 serial bus. In this manner, the present invention provides for the use of more direct communication technologies, such as the IEEE 1394 serial bus, while simultaneously providing a greater degree of security than previously available. Furthermore, greater reliability is provided because the processor of the computer being controlled does not act as an intermediary for management commands. Further still, the present invention allows management commands and normal data traffic to be conveyed using the same communication medium. These and other

advantages and features of the subject invention will become apparent from the detailed description of the invention that follows.

Brief Description Of The Drawings

5 In the detailed description of presently preferred embodiments of the present invention which follows, reference will be made to the drawings comprised of the following figures, wherein like reference numerals refer to like elements in the various views and wherein:

FIG. 1 is a schematic block diagram of a conventional general-purpose digital computing environment that can be used to implement various aspects of the present invention;

10 FIG. 2. is a schematic block diagram of a computer system to which the present invention may be beneficially applied;

FIG. 3 is a flow chart illustrating a method for controlling a computer in accordance with the present invention; and

15 FIG. 4 is a schematic block diagram of an implementation of the present invention based on a computer-readable medium.

Detailed Description of the Invention

20 The present invention may be more fully described with reference to FIGS. 1-4. FIG. 1 is a schematic diagram of a conventional general-purpose digital-computing environment that can be used to implement various aspects of the present invention. A computer 100 includes a processing unit 110, a system memory 120 and a system bus 130 that couples various system components including the system memory to the processing unit 110. The system bus 130 may be any of several types of bus structures including a memory bus or memory controller, a peripheral bus, and a local bus using any of a variety of bus architectures. The system memory 25 120 includes a read only memory (ROM) 140 and a random access memory (RAM) 150.

A basic input/output system (BIOS) 160 (or other firmware model, such as the so-called Extensible Firmware Interface; collectively referred to as platform firmware) containing the basic routines that help to transfer information between elements within the computer 100, such

as during start-up, is stored in ROM 140. The computer 100 also includes a hard disk drive 170 for reading from and writing to a hard disk (not shown), a magnetic disk drive 180 for reading from or writing to a removable magnetic disk 190, and an optical disk drive 191 for reading from or writing to a removable optical disk 192, such as a CD ROM or other optical media. Hard disk 5 drive 170, magnetic disk drive 180, and optical disk drive 191 are respectively connected to the system bus 130 by a hard disk drive interface 192, a magnetic disk drive interface 193, and an optical disk drive interface 194. The drives and their associated computer-readable media provide nonvolatile storage of computer readable instructions, data structures, program modules and other data for the computer 100. It will be appreciated by those skilled in the art that other 10 types of computer readable media which can store data that is accessible by a computer, such as magnetic cassettes, flash memory cards, digital video disks, Bernoulli cartridges, random access memories (RAMs), read only memories (ROMs), and the like, may also be used in the exemplary operating environment.

A number of program modules can be stored on the hard disk, magnetic disk 190, optical disk 192, ROM 140 or RAM 150, including an operating system 195, one or more application programs 196, other program modules 197, and program data 198. In particular, the RAM 150 will, from time to time, store various device drivers, as known in the art. A user can enter commands and information into computer 100 through input or selection devices, such as a keyboard 101 and a pointing device 102. Alternatively, a user can enter commands and information on a remote computer which commands are then converted to management commands communicated to the computer via communication buses such as LAN, WAN or IEEE 1394 serial bus. The pointing device 102 may comprise a mouse, touch pad, touch screen, voice control and activation or other similar devices. Other input devices (not shown) may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other 15 input devices are often connected to the processing unit 110 through a serial port interface 106 that is coupled to the system bus, but may be connected by other interfaces, such as a parallel port, a game port or a universal serial bus (USB). A monitor 107 or other type of display device 20 is also connected to system bus 130 via an interface, such as a video adapter 108. In addition to

the monitor, personal computers typically include other peripheral output devices (not shown), such as speakers and printers.

A serial interface in the form of an IEEE 1394 interface 140 is preferably provided. The IEEE 1394 interface 140 couples an IEEE 1394-compliant serial bus 145 to the system bus 130 or similar communication bus. The IEEE 1394-compliant serial bus 145, as known in the art, allows multiple devices 150 to communicate with the computer 100 and each other using high-speed serial channels and, in particular, allows other devices coupled to the serial bus to have direct access to various of the computer's 100 components.

The computer 100 can operate in a networked environment using logical connections to one or more remote computers, such as a remote computer 109. The remote computer 109 typically includes at least some of the elements described above relative to the computer 100, although only a memory storage device 111 has been illustrated in FIG. 1. The logical connections depicted in FIG. 1 include a local area network (LAN) 112 and a wide area network (WAN) 113. Such networking environments are commonplace in offices, enterprise-wide computer networks, intranets and the Internet.

When used in a LAN networking environment, the computer 100 is connected to local network 112 through a network interface or adapter 114. When used in a WAN networking environment, the computer 100 and remote computer 109 may both include a modem 115 or other means for establishing a communications over wide area network 113, such as the Internet. The modem 115, which may be internal or external, is connected to system bus 130 via the serial port interface 106. In a networked environment, program modules depicted relative to the computer 100, or portions thereof, may be stored in the remote memory storage device.

It will be appreciated that the network connections shown are exemplary and other means of establishing a communications link between the computers can be used. The existence of any of various well-known protocols, such as TCP/IP, "ETHERNET", FTP, HTTP and the like, is presumed, and the system can be operated in a client-server configuration to permit a user to retrieve web pages from a web-based server.

Referring now to FIG. 2, there is illustrated a schematic block diagram of a computer system 200 to which the present invention may be beneficially applied. In particular, the computer system 200 comprises a computer 202 coupled via a communication bus to a plurality of devices 204-212, labeled Device A-E. The computer 202 can be a computer as illustrated in FIG. 1. Likewise, the devices 204-212 may also be such computers, or may be specialized devices capable of communicating via the communication bus.

In a preferred embodiment, the communication bus comprises an IEEE 1394 serial bus. To this end, the computer 202 and each of the devices 204-212 comprises an interface 220 (shown only for the computer 202) that implements the IEEE 1394 protocol. Each interface 220 functionally constitutes a node, as that term is used in IEEE 1394, which in turn supports one or more ports. In general, the device to which a node is coupled acts as the "local host" for that node. For example, the computer 202 is the local host for a node implemented by the interface 220. It is not necessary for every node to have a local host, nor is it necessary that the local host always be powered. Each of the nodes may have identical construction, although some of the nodes can be simplified because of their specific functions. Thus, the nodes can be modified to meet the needs of the particular local host. For example, the node having the computer 202 as its local host, as illustrated, has three ports 222a-c; "Device A" and "Device D" each support two ports, labeled with reference numerals 224a-b and 230a-b, respectively; and "Device B", "Device C" and "Device E" each support only one port, labeled with reference numerals 226, 228 and 232, respectively.

A particular feature of the present invention is the use of a management port. As used herein, a management port is a predetermined port supported by a node for the benefit of the node's local host, which port is deemed the only port authorized to receive management commands from devices coupled to the communication bus. A management command is any type of message, request or command received from any device coupled to the communication bus relating to remote management, including attempts to read data from or write data to internal components of the computer being controlled. Examples of management commands include, but are not limited to, "system reset", "system power down", "system power up", "read status" (from

a given device), “read/set configuration” (of a specific device or of the system as a whole), etc. For example, the computer 202 shown in FIG. 2 comprises a single management port 222c. Thus, only management commands received from at least one of the devices 210, 212 coupled to the management port 222c are given consideration by the computer 202. Operations of the 5 computer 202 and interface 220 as they pertain to the present invention are more fully described with reference to FIG. 3.

Referring now to FIG. 3, at step 302, the computer identifies all devices coupled to its ports and, more particularly, which devices are authorized management devices. In a preferred embodiment, an authorized management device can only be a device coupled, either directly or 10 indirectly, to a management port of the computer. For example, “Device D” in FIG. 2 is coupled directly to the management port 222c, whereas “Device E” is indirectly coupled to the management port 222c. As its name would imply, an authorized management device is any device coupled to the communication bus that is authorized to issue management commands, e.g., a remote management terminal. A management port is a predetermined port (for example, 15 as designated by configuration data entered by a user or through a standardized assumption) that is assumed to be trusted from a security viewpoint.

In a preferred embodiment, the communication bus is an IEEE 1394 serial bus. In this case, step 302 is preferably implemented in accordance with the method taught in co-pending U.S. Patent Application Serial No. 09/515,424 entitled “METHOD AND APPARATUS FOR 20 PROVIDING SECURE REMOTE DEBUGGING OF COMPUTER SOFTWARE OVER A SERIAL BUS”. As taught therein, an IEEE 1394 bus manager (implemented at least in part by, e.g., the interface 220) generates a topology map based on the self-identification packets issued by each device after a reset of the serial bus. The topology map illustrates the hierarchy of devices coupled to each port of a given device, e.g., the computer 202 being controlled. Where 25 the computer being controlled and its corresponding interface support the bus manager, the map is readily available for use. If however, another device implements the bus manager through its corresponding interface, the topology map may be provided to the computer being controlled, either by “pushing” the map to the computer being controlled or by simply allowing the

computer to access the map when necessary. Based on the topology map, the interface on the computer being controlled can determine which devices are coupled to its management port, and which devices are therefore authorized. Those having ordinary skill in the art will recognize that further criteria may be used to determine authorized management devices. For example, only 5 devices directly coupled to the management port may be authorized. As another example, only devices a certain number of "hops" away from the management port (i.e., devices indirectly coupled to the management port through at least a given number of intermediary devices) may be authorized.

Regardless, at step 304, it is determined whether the computer has received a 10 management command. In the preferred case of IEEE 1394, this determination is made by the interface by inspecting the received data. Step 304 is continuously repeated if no such management command is received. When a management command is received, processing continues at step 306 where it is determined whether the management command was received from an authorized device. If, at step 306, it is determined that the management command was 15 not received from an authorized device, the management command is ignored and processing continues at step 304. Again, in the preferred case of IEEE 1394, these steps are performed by the 1394 interface based on its knowledge of the topology map described above and the predetermined identity of the management port. Thus, the received management command is inspected to determine its source identification. The source identification is then compared with 20 identifications of authorized devices as determined by the topology map and knowledge of the management port identification.

The technique described above relies on knowledge of the source identification of a received command to determine whether an authorized management device sent the command. In an alternative embodiment, rather than relying on source identification to ascertain 25 authorization, it may be preferable to rely only upon knowledge of the receiving port's identification. Such a technique necessarily depends on the ability of the device being managed to discriminate, for each management command received, the identity of a corresponding receiving port. For example, this could be inherently done where each receiving port has its own

separate received data buffer. Thus, it is understood that data stored in a particular port's buffer has been received over that port. Alternatively, such identification could be explicit. For example, a protocol stack or similar functionality within the device being managed could cause a port identification to be appended to each received management command. In this manner, 5 simple inspection of the appended data will determine the receiving port's identification. Where this alternative technique is used, the processing described relative to step 302 need not be performed since source identification is no longer used. Likewise, step 306 need not rely upon a topology map and instead simplifies to ascertaining the identification of the port through which a management command was received and comparing that identification with the known 10 identification of the management port.

If the management command was received from an authorized device, regardless of the manner in which it was determined, processing continues at step 308 where the management command is executed. Generally, management commands may be separated into two categories, those that require participation of the device's controlling processor on behalf of the device being controlled and those that do not. In the first category are those commands, for example, inquiring about the status of a given component within the device being managed, which component can only be tested by the device's controlling processor. The second category includes, for example, management commands that seek only to inspect or alter certain memory locations within the computer's memory requiring no, or only indirect, intervention on the part of the device's controlling processor. This categorization of management commands is particularly well supported by IEEE 1394-compliant communication busses. In the IEEE 1394 context, commands in the first category are passed on to the host for execution, whereas commands in the second category are instead implemented by the IEEE 1394 interface without intervention by the host. In a preferred IEEE 1394 implementation, differentiation between the two types of 15 management commands is achieved, at least in part, through use of asynchronous and isochronous channels. In particular, management commands that do not require host intervention are sent via an asynchronous channel via the management port, whereas 20

management commands requiring host intervention are sent via an isochronous channel via the management port.

Regardless, at step 310, data may be provided to one or more devices coupled to the communication bus (or through any other output path, e.g., a monitor or network connection) in response to the management command. For example, data may be provided to the authorized management device that issued the management command. Alternatively, the management command may require that data be sent to one or more devices other than the authorized management device. Once again, the type of data sent at step 310 is dependent upon the type of management command executed.

Processing continues at step 312 where it is determined whether a reconfiguration event has occurred. A reconfiguration event in the context of the present invention is an event indicative of the fact that the topology of devices coupled to the computer has changed in some manner, thereby necessitating that the computer again identify the devices coupled to the communication bus. Note that although this step is illustrated as occurring at a given point within a sequence of steps, it is understood that a reconfiguration event could occur at any time and detection of such an event can likewise occur at any time. Where the communication bus is an IEEE 1394 serial bus, the configuration event is preferably a bus reset as determined by the 1394 interface. Such bus resets may be generated on command by a device coupled to the bus, or certain physical events, such as the addition or removal of a device, may automatically trigger a bus reset. Regardless, if no such reconfiguration event is detected, processing continues at step 304 where further management commands are awaited. If, however, a reconfiguration event is detected, processing continues at step 302 where the processing of identifying devices, particularly authorized management devices, is repeated. Note that where the alternative technique, described above, for determining whether a management command is authorized (i.e., through the use of the receiving port's identification alone) is used, step 312 becomes unnecessary. In this case, processing instead continues at step 304.

FIG. 4 is a schematic block diagram of an implementation of the present invention based on a computer-readable medium. The computer-readable medium 400 may comprise a hard disk,

removable magnetic disks, optical disks, magnetic cassettes, flash memory cards, Bernoulli cartridges, RAMs, ROMs, and the like. It will be appreciated by those skilled in the art that other types of computer-readable media that can store data and/or computer-executable instructions that are accessible by a computer may also be used. Regardless, the computer-readable medium 400 provides nonvolatile storage of computer-readable instructions, data structures, program modules and other data.

The computer-readable medium 400 includes a bus interface component 402, a management command authorization component 404 and a host interface component 406. Each of the components preferably comprises computer-executable instructions. As those having ordinary skill in the art will readily appreciate, various other component arrangements can be devised that encompass the same functionality. The bus interface component 402 supports communications with a communication bus (not shown) and, in particular, routes received management commands to the management command authorization component 404. Additionally, the bus interface component 402 can also send (on behalf of the computer or other device being controlled remotely) data responsive to one or more authorized management commands to devices residing on the communication bus. Such data may be provided to the bus interface component 402 without the intervention of the management command authorization component 404. This is illustrated in FIG. 4 by the arrow from the host interface component 406 to the bus interface component 402. Regardless, in a preferred embodiment, the bus interface component 402 supports communications with an IEEE 1394-compliant serial bus.

The management command authorization component 404 receives one or more management commands from the bus interface component 402 and, using the techniques described above, determines whether such management commands are authorized. If not authorized, the management commands are ignored. If authorized, the management commands are sent to the host interface component 406. Those having ordinary skill in the art will recognize that various functional aspects of the bus interface component 402 may be incorporated into the management command authorization component 404 or vice versa as a matter of design choice.

The host interface component 406 supports communications with the host of the device being controlled. In the context of the present invention, this particularly includes sending appropriate authorized management commands to the host for execution or, when necessary, executing authorized management commands directly. Additionally, when necessary, the host 5 interface component 406 receives data responsive to one or management commands and routes such data to the bus interface component. Once again, those having ordinary skill in the art will recognize that some or all of the functionality encompassed by the host interface component 406 may be incorporated into another component.

Using the techniques described herein, direct access technologies, such as the IEEE 1394 10 serial bus, may be applied to remote management systems. Using a management port, authorized management devices may be identified such that only management commands received from authorized management devices are executed, while all such other management commands are ignored. In the context of a preferred IEEE 1394 implementation, topology maps are built in response to bus resets, thereby allowing the 1394 interface to identify which devices are connected to which physical ports and to which logical ports, such as a management port. Based 15 on this knowledge, the logical management port can be correlated with a physical management port, which correlation may be communicated to users. In turn, secure remote management operations may be implemented by instructing users that, e.g., "The 1394 port closest to the back of the computer [or identified in some other manner] is the management/debug port. Only devices plugged into this port will be allowed to perform management/debug operations. Only 20 trusted devices should be plugged into this port. Any other device may safely be plugged into the other ports." Using the present invention, greater reliability is provided because the processor of the computer being controlled does not act as an intermediary for management commands. Further efficiencies are realized in that management commands and normal data traffic are 25 conveyed using the same communication medium.

While the foregoing detailed description sets forth presently preferred embodiments of the invention, it will be understood that many variations may be made to the embodiments disclosed herein without departing from the true spirit and scope of the invention. This true spirit

MS 148611.2
BW 03797.85750

and scope of the present invention is defined by the appended claims, to be interpreted in light of the foregoing specifications.

Claims

What is claimed is:

1. A method for remotely managing a computer coupled to a communication bus, the method comprising:

5 receiving, via the communication bus, a management command;

determining whether the management command was received via a management port coupled to the communication bus; and

when the management command was received via the management port, executing the management command.

10

2. The method of claim 1, further comprising:

providing, via the communication bus, data to at least one device coupled to the communication bus in response to the step of executing the management command.

15

3. The method of claim 1, further comprising:

when the management command was not received via the management port, ignoring the management command.

20

4. The method of claim 1, wherein the communication bus is an IEEE 1394-compliant serial bus.

5. A computer-readable medium having stored thereon computer executable instructions for performing the method of claim 1.

25

6. A computer-readable medium having stored thereon computer executable instructions for performing the method of claim 2.

MS 148611.2
BW 03797.85750

7. A computer-readable medium having stored thereon computer executable instructions for performing the method of claim 3.

8. A method for remotely managing a computer coupled to a communication bus, the method comprising:

identifying one or more authorized management devices based on the one or more authorized management devices being connected, via the communication bus, to a first port of the computer;

receiving a management command from a first device via the communication bus;

determining whether the first device is one of the one or more authorized management devices; and

when the first device is one of the one or more authorized management devices,

executing the management command.

9. The method of claim 8, wherein the step of identifying is performed subsequent to a reset of the communication bus.

10. The method of claim 8, further comprising:

providing, via the communication bus, data to at least one device coupled to the communication bus in response to the step of executing the management command.

11. The method of claim 8, further comprising:

receiving another management command from a second device via the communication bus;

determining whether the second device is one of the one or more authorized management devices; and

when the second device is not one of the one or more authorized management devices,

ignoring the other management command.

12. The method of claim 8, wherein the communication bus is an IEEE 1394-compliant serial bus.

13. A computer-readable medium having stored thereon computer executable instructions for performing the method of claim 8.
- 5 14. A computer-readable medium having stored thereon computer executable instructions for performing the method of claim 10.
15. A computer-readable medium having stored thereon computer executable instructions for performing the method of claim 11.

10

16. A computer comprising:

a processor;

an IEEE 1394 interface, coupled to the processor, comprising at least one port wherein the IEEE 1394 interface passes management commands received from a management port of the at least one port to the processor and ignores any management command received via any port of the at least one port other than the management port; and

memory, coupled to the processor, having stored thereon computer executable instructions that, when executed by the processor, cause the computer to:

execute at least one management command received via the management port.

10

17. The computer of claim 16, wherein the computer executable instructions, when executed by the processor, further cause the computer to:

provide data via any of the at least one port in response to the at least one management command received via the management port.

15

18. The computer of claim 16, wherein the computer executable instructions, when executed by the processor, further cause the computer to:

identify one or more authorized management devices coupled to the management port.

20

19. A system comprising the computer of claim 16, and further comprising:

an IEEE 1394-compliant serial bus coupled to the IEEE 1394 interface; and

a management device coupled, via the IEEE 1394-compliant serial bus, to the management port,

wherein the management device provides the at least one management command.

25

20. The system of claim 19, wherein the management device is another computer.

21. A computer-readable medium comprising computer-executable components for enabling remote management of a computer via a communication bus, the computer-executable components comprising:

a bus interface component that communicates with the communication bus and that

5 receives one or more management commands via the communication bus; and

a management command authorization component, in communication with the bus interface component, that determines whether each of the one or more management commands is authorized based on whether each of the one or more management commands was received via a management port coupled to the communication bus.

10

22. The computer-readable medium of claim 21, wherein the bus interface component communicates with an IEEE 1394-compliant serial bus.

23. The computer-readable medium of claim 21, further comprising:

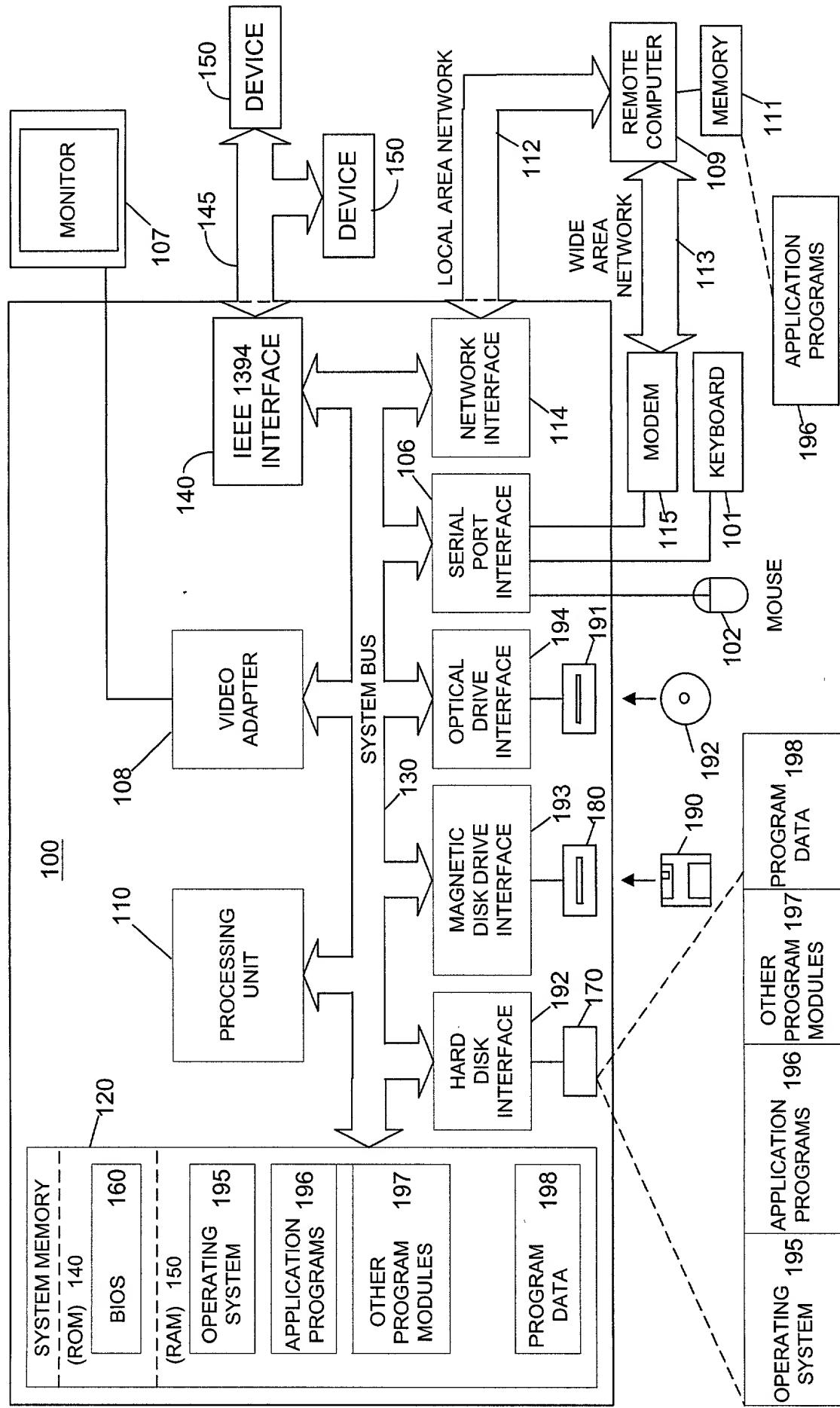
15 a host interface component, in communication with the management command authorization component and a host comprising a portion of the computer, that sends the one or more management commands to the host for execution when the one or more management commands are authorized and require host intervention.

20 24. The computer-readable medium of claim 23, wherein the host interface component executes the one or more management commands when the one or more management commands are authorized and do not require the intervention of the host.

25 25. The computer-readable medium of claim 23, wherein the host interface component does not send the one or more management commands to the host when the one or more management commands are not authorized.

Abstract of the Disclosure

A computer being controlled is coupled via a communications bus to at least one other device comprising one or more authorized management devices. The one or more authorized management devices are coupled to a management port. Only management commands received 5 from authorized management devices via the management port may be executed or otherwise responded to. Management commands received from other devices are ignored. In a preferred embodiment, the communication bus is an IEEE 1394 serial bus. In this manner, the present invention provides for the use of more direct communication technologies, such as the IEEE 394 serial bus, while simultaneously providing a greater degree of security than previously available.



1

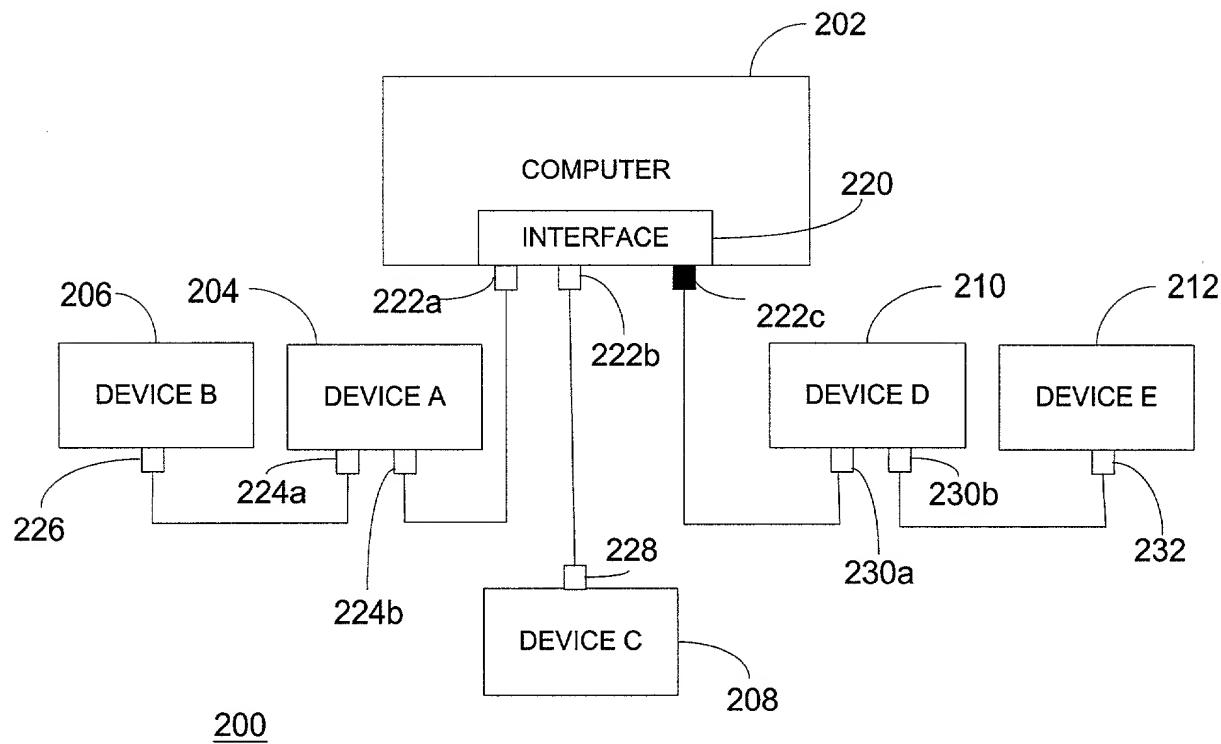


FIG. 2

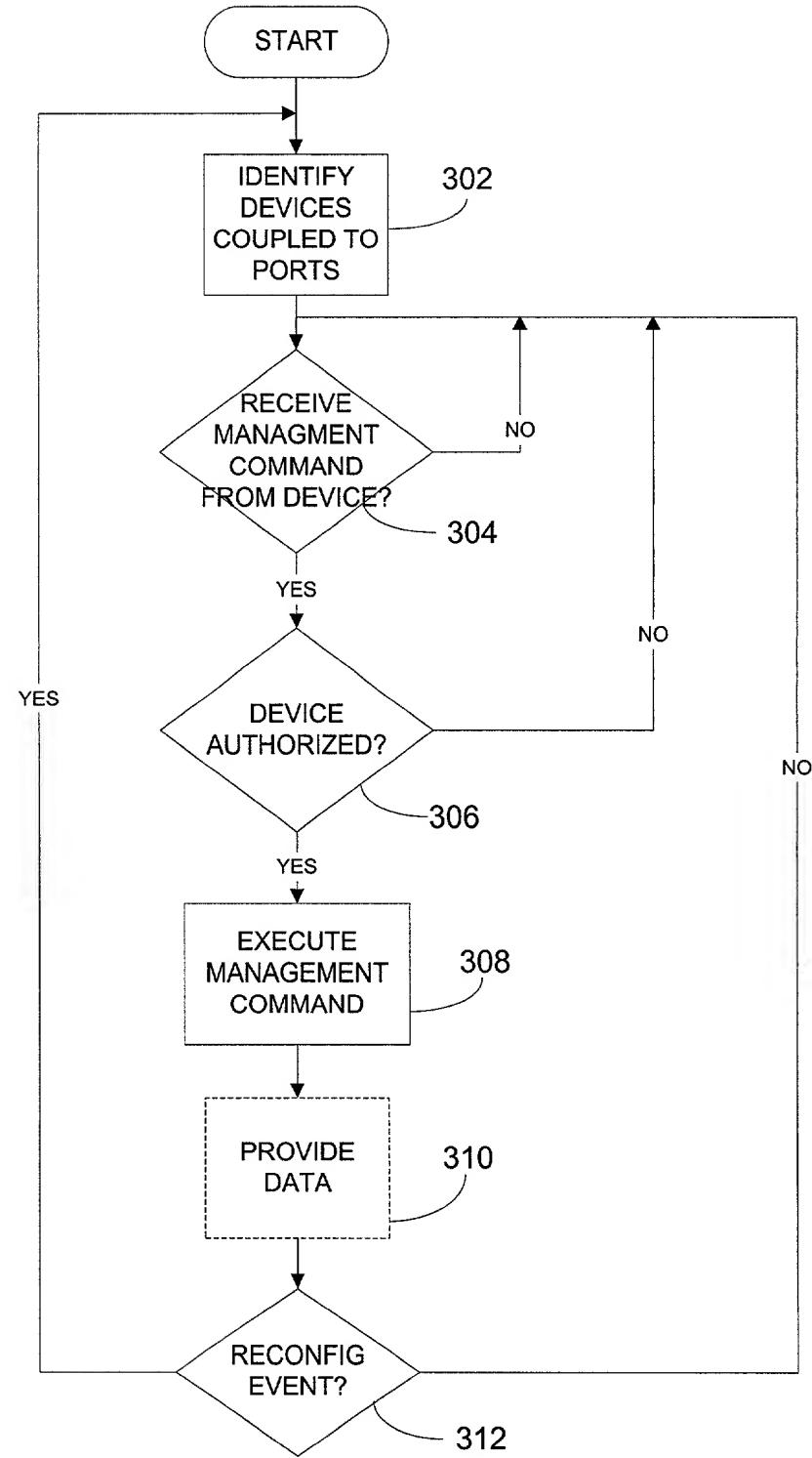


FIG. 3

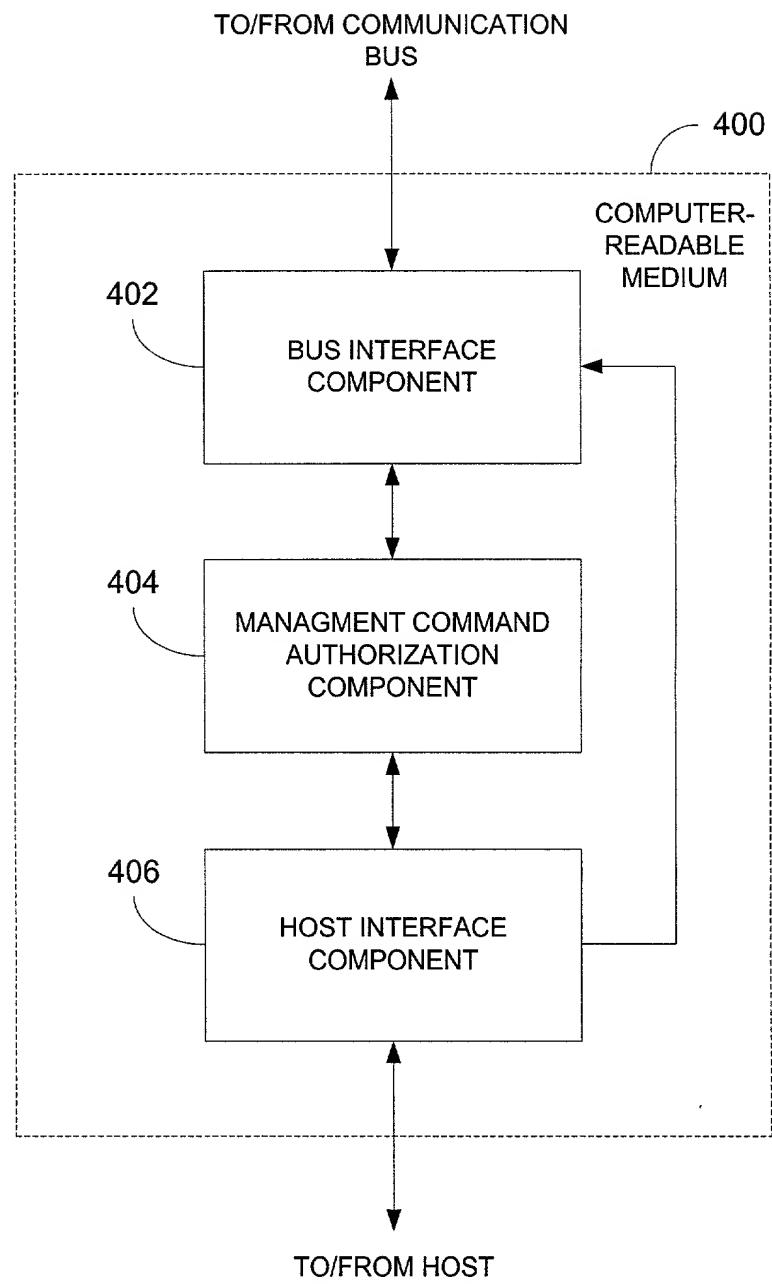


FIG. 4

JOINT DECLARATION FOR PATENT APPLICATION

As the below named inventor, we hereby declare that:

Our residence, post office address and citizenship are as stated below next to our names;

We believe we are the original, first and joint inventors of the subject matter which is claimed and for which a patent is sought on the invention entitled Method And Apparatus Of Remote Computer Management, the specification of which

- is attached hereto.
- was filed on _____ as Application Serial Number _____ and was amended on _____ (if applicable).
- was filed under the Patent Cooperation Treaty (PCT) and accorded International Application No. _____, filed _____, and amended on _____ (if any).

We hereby state that we have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

We hereby acknowledge the duty to disclose information which is material to patentability in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Prior Foreign Application(s)

We hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

Country	Application No.	Date of Filing (day month year)	Date of Issue (day month year)	Priority Claimed Under 35 U.S.C. §119

Prior United States Provisional Application(s)

We hereby claim priority benefits under Title 35, United States Code, §119(e)(1) of any U.S. provisional application listed below:

U.S. Provisional Application No.	Date of Filing (day month year)	Priority Claimed Under 35 U.S.C. §119(e)(1)
60/169,718	08 December 1999	Yes

Prior United States Application(s)

We hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, we acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

Application Serial No.	Date of Filing (Day, Month, Year)	Status — Patented, Pending, Abandoned
09/515,424	29 February 2000	Pending

Power of Attorney

And we hereby appoint, both jointly and severally, as our attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith the following attorneys and agents, their registration numbers being listed after their names:

ALTHERR, Robert F.	31,810	HONG, Patricia E.	34,373	NELSON, Jon O.	24,566
BANNER, Donald W.	17,037	HOSCHEIT, Dale H.	19,090	NIEGOWSKI, James A.	28,331
BANNER, Mark T.	29,888	HYMEL, Lin J.	245,414	PATEL, Binal J.	42,065
BANNER, Pamela I.	33,644	IWANICKI, John P.	34,628	PATHAK, Ajay S.	38,266
BECKER, Matthew P.	45,824	JACKSON, Thomas H.	29,808	PAYNE, Stephen S.	35,316
BECKETT, William W.	18,262	KAGAN, Sarah A.	32,141	PETERSON, Thomas L.	30,969
BERGHAMMER, Joseph J.	46,057	KATZ, Robert S.	36,402	POTENZA, Joseph M.	28,175
BODNER, Jordan	42,338	KLEIN, William J.	43,719	PRATT, Thomas K.	37,210
BUROW, Scott A.	42,373	KRAUSE, Joseph P.	32,578	RENK, Christopher J.	33,761
CALLAHAN, James V.	20,095	LINEK, Ernest V.	29,822	RESIS, Robert H.	32,168
CHANG, Steve S.	42,402	MALONE, Dale A.	32,155	RIVARD, Paul M.	43,446
COHAN, Gregory J.	40,959	MANNAVA, Ashok K.	45,301	SCHAD, Steven P.	32,550
COOPERMAN, Marc S.	34,143	MAPLE, Marie-Claire B.	37,588	SHIFLEY, Charles W.	28,042
CURTIN, Joseph P.	34,571	MAY, Steven A.	44,912	SKERPON, Joseph M.	29,864
DAWSON, John R.	39,504	McDERMOTT, Peter D.	29,411	SPAR, Elizabeth	45,123
DEMOOR, Laura J.	39,654	McKEE, Christopher L.	32,384	STOCKLEY, D. J.	34,257
EVANS, Thomas L.	35,805	McKIE, Edward F.	17,335	VAN ES, J. Pieter	37,746
FEDOROCHKO, Gary D.	35,509	MEDLOCK, Nina L.	29,673	WITCOFF, Sheldon W.	17,399
FISHER, Daniel E.	34,162	MEECE, Timothy C.	38,553	WOLFFE, Franklin D.	19,724
FISHER, William J.	32,133	MEEKER, Frederic M.	35,282	WOLFFE, Susan A.	33,568
GLEMBOCKI, Christopher R.	38,800	MILLER, Charles L.	43,805	WRIGHT, Bradley C.	38,061
HANLON, Brian E.	40,449	MITRIUS, Janice V.	43,808	SAKO, Katie E.	32,628
HEMENDINGER, Lisa M.	42,653	MORENO, Christopher P.	38,566	CROUSE, Daniel D.	32,022

All correspondence and telephone communications should be addressed to:

Pamela I. Banner

Banner & Witcoff, Ltd.
1001 G Street, N.W., 11th Floor
Washington, D.C. 20001-4597

Customer Number: 22907

Tel: (202) 508-9100

Fax: (202) 508-9299

We hereby declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Signature Chrysanthakopoulos Date 9/25/2000
 Full Name of First Inventor Chrysanthakopoulos First Given Name Georgios Second Given Name -
 Family Name - Citizenship Greece
 Residence Kirkland, Washington Post Office Address 715 7th Street South, Kirkland, Washington 98033

Signature DeMaio Date 9/25/00
 Full Name of Second Inventor DeMaio First Given Name Pasquale Second Given Name -
 Family Name - Citizenship United States of America
 Residence Bellevue, Washington Post Office Address 16817 SE 3rd Place, Bellevue Washington 98008

O Additional Inventor(s) named on next page.

Signature Valerie R. See Date 9/26/00
Full Name of Third Inventor See Family Name Valerie First Given Name Valerie Second Given Name R.
Residence Snohomish, Washington Citizenship United States of America
Post Office Address 19410 Lerch Road, Snohomish, Washington 98290